

AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A computer-implemented process for receiving from a plurality of sending clients media data packets across a firewall sent to a single destination address and a single destination port of a firewall, comprising the process actions of:

establishing a plurality of security associations (SAs) for dialogs between sending clients and receiving clients, each SA including source information of a sending client and an indication of a receiving client;

receiving from ~~the~~ a sending client an encrypted media packet sent using Real-time Transport Protocol (RTP) message format at a media-relay server, the encrypted media packet being sent to the ~~wherein a destination address and a the destination port of multiple receiving network clients are not unique from the perspective of a sending client;~~

determining whether the sending client's Security Association (SA) exists using the sender's source information received with the media packet ~~included in the RTP message header;~~

if no SA exists, dropping the media packet at the media-relay server; and
if a SA does exist, decrypting the media packet;

obtaining a Synchronization Source Identifier (SSRC) from the SA;

comparing the Synchronization Source Identifier included in the decrypted RTP media packet with the Synchronization Source Identifier obtained from the SA;

if the Synchronization Source Identifier included in the decrypted RTP packet does not match the Synchronization Source Identifier obtained from the SA, dropping the media packet; and

if the Synchronization Source Identifier in the decrypted RTP ~~packet~~ matches to the Synchronization Source Identifier obtained from the

SA, forwarding the packet to a receiving ~~network-client-identified~~
indicated in the SA-based on the sender's source information
wherein a plurality of sending clients send media packets to the
destination address and the destination port.

2. (Original) The computer-implemented process of Claim 1 wherein the source information retrieved by the media-relay server comprises a source Internet Protocol (IP) address and port number found in the RTP message format.

3. (Original) The computer-implemented process of Claim 1 wherein the media packet comprises audio data.

4. (Original) The computer-implemented process of Claim 1 wherein the media packet comprises video data.

5-16. (Cancelled)

17. (New) A method in a media-relay server for relaying to receiving clients packets of a real-time transport protocol received from sending clients through a single destination address and a single destination port of a firewall, the method comprising:

for each of a plurality of sending clients, establishing a security association for a dialog between the sending client and a receiving client, the security association including an encryption key for decrypting packets sent from the sending client to the receiving client via the destination address and the destination port, a synchronization source identifier that uniquely identifies the sending client within the dialog, source information of the sending client, and an indication of the receiving client;

receiving from a sending client a datagram of a user datagram protocol sent to the destination address and the destination port, the datagram including an encrypted packet and source information of the sending client; and upon receiving the datagram,

- when no security association has been established that includes the source information of the received datagram, dropping the encrypted packet; and
- when a security association has been established that includes the source information of the received datagram, decrypting the encrypted packet using the encryption key of the established security association;
- when the synchronization source identifiers of the decrypted packet and the established security association do not match, dropping the decrypted packet; and
- when the synchronization source identifiers of the decrypted packet and the established security association do match, forwarding the decrypted packet to the receiving client indicated in the established security association.

18. (New) The method of claim 17 including receiving from each of the plurality of sending clients datagrams sent to the destination address and the destination port.

19. (New) The method of claim 17 wherein the media-relay server is connected to a external firewall through which datagrams are received from sending clients and an internal firewall through which packets are forwarded to receiving clients.

20. (New) The method of claim 17 wherein the source information is a source address and a source port of the datagram.

21. (New) The method of claim 17 wherein the source information is a synchronization source identifier of the datagram.

22. (New) The method of claim 17 wherein the source information of the datagram is not encrypted.

23. (New) A media-relay server for relaying to receiving clients packets of a real-time transport protocol received from sending clients through a single destination address and a single destination port of a firewall, the media-relay server comprising:

security associations established for sending clients and receiving clients, the security association for a sending client including, a synchronization source identifier that uniquely identifies the sending client within the dialog, source information of the sending, and an indication of the receiving client;

a component that receives from a sending client an encrypted packet of the real-time transport protocol and source information of the sending client sent by the sending client to the destination address and the destination port; and

a component that

when no security association has been established that includes the received source information, drops the encrypted packet; and

when a security association has been established that includes the received source information,

decrypts the encrypted packet;

when a synchronization source identifier of the decrypted packet and a synchronization source identifier the established security association do not match, drops the decrypted packet; and

when the synchronization source identifier of the decrypted packet and the synchronization source identifier of the established security association do match, forwards the decrypted packet to the receiving client indicated in the established security association.

24. (New) The media-relay server of claim 23 wherein packets are received from each of the plurality of sending clients sent to the destination address and the destination port.

25. (New) The media-relay server of claim 23 wherein the media-relay server is connected to a external firewall through which encrypted packets are received from sending clients and an internal firewall through which decrypted packets are forwarded to receiving clients.

26. (New) The media-relay server of claim 23 wherein the source information is a source address and a source port of the datagram.

27. (New) The media-relay server of claim 23 wherein the source information is a synchronization source identifier of the datagram.

28. (New) The media-relay server of claim 23 wherein the source information of the datagram is not encrypted.